

Notice of Allowability

Application No.

09/661,049

Examiner

Abdulkhikim Nobahar

Applicant(s)

SPIES, TERENCE R.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 02/13/2006.
2. ☒ The allowed claim(s) is/are 83-124.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |

DETAILED ACTION

1. This communication is in response to applicant's response received on February 13, 2006.
2. Claims 1 to 82 are cancelled.

Allowable Subject Matter

1. Claims 83-124 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the independent claims 83, 92, 97, 106, 111 and 120 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior arts are Hardy et al. (6,079,018; hereinafter Hardy) and Epstein (6,453,416 B1). Hardy discloses a method and a system for digitally signing a document by applying a predefined one-way hash function to the document. Hardy also discloses that a value, K1, is generated and this value is combined with a hash value of a document, H, which is generated by a hashing procedure in order to produce an intermediate value, K2. Epstein teaches a secure signing device and a method for using such a device to create a digital signature. Epstein further teaches that a number of data strings are provided by a

Art Unit: 2132

computer system and hash of one of the data is computed. However, these three arts, singularly or in combination, fail to anticipate or render the following limitation:

“Claims 83 and 97: building a data block comprising a first random value and a cryptographic hash of the first random value;

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.”

“Claims 92 and 106: accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.”

“Claim 111: means for building a data block comprising a first random value and a cryptographic hash of the first random value;

means for computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.”

"Claim 120: means for accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

means for computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value."

3. The dependent claims 84-91, 93-96, 98-105, 107-110, 112-119 and 121-124 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

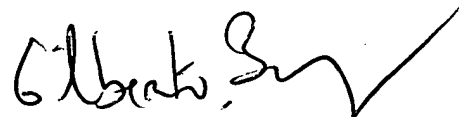
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner

Art Unit 2132 *A.N.*

March 30, 2006



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100